European Economic and Social Committee

TEN/631
Protection of personal data

OPINION

European Economic and Social Committee

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
[COM(2017) 10 final – 2017/0003 (COD)]

Rapporteur: **Laure BATUT**

Referral	European Parliament, 16/02/2017 Council of the European Union, 09/03/2017
Legal basis	Articles 16 and 114 of the Treaty on the Functioning of the European Union
Section responsible	Section for Transport, Energy, Infrastructure and the Information Society
Adopted in section	14/06/2017
Adopted at plenary	05/07/2017
Plenary session No	527
Outcome of vote (for/against/abstentions)	155/0/5

1. Conclusions and recommendations

1.1 The EESC regrets very much that these texts are voluminous and entangled, and that to understand them it is necessary to go back and forth between them, such that it is unlikely that anyone other than a select few will ever read and apply them and that their added value is not evident to the public, a principle that is missing from the entire proposal for a regulation. We recommend that a factsheet be published online with a description of the texts for the general public which makes them accessible for everyone.

1.2 The EESC notes that from the options proposed in the impact assessment the Commission has chosen the one that would entail "measured" reinforcement of privacy. Is this to guarantee a balance with the interests of industry? The Commission does not specify which aspects of a "far reaching" reinforcement of privacy would have harmed industry interests. This position has the effect of already watering down the proposal at the drafting stage.

1.3 The EESC recommends that the Commission:

1) consider that, henceforth, everything can become a piece of data and be the subject of electronic communication, with repercussions for the privacy of natural and legal persons;
2) clarify the proposal's application of the Charter of Fundamental Rights and human rights (in Articles 5, 8 and 11), as well as the possibilities for restriction introduced by national legislation (Recital 26);
3) Review Articles 5 and 6 of the proposal. In allowing electronic communications, the internet and mobile telephony are services of general interest to which access must be universal, available and affordable, without consumers being forced to consent to their data being processed as a requirement imposed by providers in order to benefit from these services. It is therefore necessary to stipulate an obligation to systematically propose to users the option of refusing cookies, tracking systems, etc., based on clear information;
4) clearly establish that the *lex specialis* proposed for completing the general data protection regulation (GDPR) respect the general principles of the afore-mentioned text and not diminish established protection, and that any processing, including web audience measuring, be subject to the principles of the GDPR (Article 8);
5) guarantee regulatory stability for the public and for businesses and, to that end, clarify the regulation's text and the content of its implementing measures in order to avoid having too many delegated acts;
6) develop a strategy which can demonstrate to all consumers that the Union is remaining faithful to its principles of respecting human rights, and that its intention is to ensure that not only electronic communications operators, but also OTT – Over-The-Top – services, respect people's privacy;
7) avoid health representing a wide open breach in protection, offering potential for the exploitation of people's privacy and personal data by electronic communications operators for the purposes of profiteering;
8) pay attention to the sharing economy, and the transfer and use of data by means of electronic communications platforms, often located outside the EU;

9) take into account the internet of things (IoT), which is most intrusive and may be a vehicle for privacy breaches when data are sent via electronic communications;
10) take account of what follows data transfer and protect the data that people store, for most of such data is private (whatever the interface, including cloud computing);
11) clarify the protection of machine-to-machine (M2M) data transfer and devote a whole article to it, not just one recital (12);
12) set up a European portal (DG Justice) that is universally accessible and comprehensible to help the public find their way through the maze of texts and exercise their rights, giving access to European and national texts, appeals procedures and case law (for example, clarifying Recital 25 and Articles 12 and 13);
13) provide the supervisory authorities with the resources needed to carry out their tasks (European Data Protection Supervisor (EDPS), national authorities);
14) allow consumers to bring class actions before the courts in order to ensure their rights are upheld at European level, by going further in a new directive than in Recommendation C(2013) 401&3539[1].

2. Aspects of the legislative context

2.1 Electronic communications networks have expanded considerably since Directives 95/46/EC and 2002/58/EC[2] on the protection of privacy of natural and legal persons in the electronic communications sector.

2.2 The **General Data Protection Regulation (GDPR) adopted in 2016** (Regulation (EU) 2016/679) became the basis for the measures concerned and laid down the main principles, including those for judicial and criminal data. In accordance with this regulation, personal data may only be compiled under strict conditions, for legitimate purposes, and respecting confidentiality (Article 5 of the GDPR).

2.2.1 In **October 2016**, the Commission presented a proposal for a European Electronic Communications Code[3] (300 pages long), which has not yet been adopted, but to which reference is made for certain definitions which are not set out in the GDPR or in the proposal in hand.

2.2.2 Two proposals dated January 2017 stipulate certain aspects which are based on the GDPR: the proposed regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies (**COM(2017) 8 final**, EESC rapporteur on this subject: Mr Pegado Liz); and the proposed regulation in hand (**COM(2017) 10 final**), on respect for private life and the protection of personal data.

1 11.06.203-IP/13/525 and Memo13/531-DG Justice.

2 Directive 2002/58/EC, amongst other things, prohibits the use of spam (Article 13) by setting up – following the 2009 modification – the opt-in principle, according to which operators must obtain the consent of recipients before sending "marketing messages".

3 COM(2016) 590 final, 12.10.2016, proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (EECC), p. 2; see OJ C 125, 21.4.2017, p. 56.

2.3 The three aforementioned texts will **apply as of the same date** – **25 May 2018** – and aim to harmonise rights and monitoring procedures.

2.4 Note that, in order to facilitate this approach, it has been decided to protect privacy using a European regulation and no longer a directive.

3. Introduction

3.1 Civil society would like to understand whether, in this all-digital world which is taking shape, the Union is bringing added value which guarantees forums where private life can thrive without fear.

3.2 Data being generated continuously means that all users are traceable and identifiable everywhere. Data processing carried out in centres which are mostly located physically outside Europe is a cause for concern.

3.3 Big Data has become a currency, and the smart processing thereof means that natural and legal persons can be "profiled", their data "marketed" and money made, often without a user's knowledge.

3.4 However, it is above all the appearance of new players in the data-processing sector, over and above internet access providers, which must lead to a review of the relevant texts.

4. Summary of the proposal

4.1 The Commission's intention with this proposal is to establish a balance between consumer and industry interests by:

- authorising the use of data by operators while allowing the end-user to keep control by giving their explicit consent;
- requiring operators to say what they intend to do with such data;
- selecting Option 3 of the impact assessment, which favours "measured" reinforcement of privacy, rather than Option 4, which would entail "far reaching" reinforcement.

4.2 The proposal is aimed at the deployment of the GDPR, which is of general application, as are confidentiality of private data and the right of erasure, with regard to the specific aspect of respect for privacy and the protection of personal data in telecommunications; the intention is to establish stricter rules for protection of privacy, as well as coordinated monitoring and penalties.

4.3 The proposal does not lay down specific measures with regard to "breaches" in personal data caused by the users themselves, but does confirm the principle of the confidentiality of electronic communications data at the outset (Article 5).

4.4 Providers may process the content of electronic communications:

- to provide a service to an end-user who has given his or her consent; or

– to provide a service to the end-users concerned (Article 6(3)(a) and (b)) who have given their consent.

4.5 They are obliged to erase the data or make it anonymous after receipt by the intended addressees.

4.6 Under Article 4(11) of the GDPR, the "consent" of a data subject means any freely given, specific, informed and unambiguous indication of that data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

4.7 The proposal maintains the requirement for **consent to be expressly given**, as defined in the GDPR, burden of proof being on the operator.

4.8 "Processing" is itself based on consent. The controller has to "be able to demonstrate that the data subject has consented to processing of his or her personal data" (GDPR Article 7(1)).

4.9 Some limitations (on obligations for and rights to) confidentiality could be provided by EU law or national law to safeguard public interest or guarantee an inspection exercise.

4.10 Natural persons must have given their consent to appearing in a publicly available directory, with the means to verify or correct the data that concern them (Article 15).

4.11 A right to object will enable all users to block the use of data concerning themselves which has been entrusted to a third party (for example a trader) and then each time a message is sent (Article 16). The new rules will give users more control over their parameters (cookies, identifiers) and unsolicited communications (spam, messages, texts, calls) will be able to be blocked if the user has not given his or her agreement.

4.12 As regards the identification and blocking of unwanted calls (Articles 12 and 14), the regulation underlines that these rights also apply to legal persons.

4.13 The structuring of a monitoring system is in accordance with the GDPR (Chapter VI on supervisory authorities and Chapter VII on cooperation between supervisory authorities).

4.13.1 It is the Member States and their national authorities responsible for data protection who will have to ensure compliance with the rules on confidentiality. Other supervisory authorities will, as part of mutual assistance, be able to draft objections that might be submitted to national supervisory authorities. They will cooperate with the latter or with the European Commission in the framework of a consistency mechanism (GDPR Article 63).

4.13.2 For its part, the European Data Protection Board (EDPB) is responsible for ensuring consistent application of the regulation in hand (GDPR Articles 68 and 70).

It may be asked to publish guidelines, recommendations and best practice so as to facilitate application of the regulation.

4.14 Remedies are possible for natural and legal persons who are final users so they can assert interests adversely affected by infringements; they may receive compensation from the infringer for damage suffered.

4.15 The amounts envisaged for administrative fines are intended to act as a deterrent, since for those offending they can be as high as ten million euros and, for firms, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 23). Where there is no provision for an administrative fine, Member States set penalties and notify the Commission thereof.

4.16 The new text on respect for privacy and the use of personal data will **apply as of 25 May 2018**: on the same date, therefore, as the 2016 GDPR and the regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies, and the proposal for a directive establishing the European Electronic Communications Code (COM(2016) 590 final), if these texts are adopted.

4.17 Scope of the lex specialis implementing the GDPR

– ***Ratione jure*: legal basis**

The legal basis is provided by TFEU Articles 16 (data protection) and 114 (single market), as well as Articles 7 and 8 of the Charter of Fundamental Rights. The regulation supplements the GDPR regarding data which can be considered as personal data.

– ***Ratione personae*: players**

These are the end-users, natural and legal persons, as defined in the draft European Electronic Communications Code, on the one side and, on the other, all the providers of communications services, not just the traditional ones, but above all new players whose new services do not offer users any guarantees. "Bypass" techniques in Over-the-Top communications services (instant messaging services, texts, Voice over IP techniques, multiple interfaces, etc.) currently fall outside the scope of existing texts.

– ***Ratione materiae*: data**

The proposal contains no provision on the retention of data in cloud computing and leaves it up to the Member States to take action, in accordance with GDPR Article 23 (restrictions on the right to object) and European Court of Justice case law (see point 1.3 of the explanatory memorandum).

Users will have to give their consent to the retention of data and metadata (date, time, location, etc.) generated in systems; failing this, the data concerned will have to be made anonymous or erased.

– ***Ratione loci*: where?**

The establishments carrying out processing activities in the EU Member States, or one of their branches located in a Member State, will be designated "leader" in monitoring activities, national monitoring authorities will play their role, and the European Data Protection Supervisor (EDPS) will supervise the whole process.

4.18 EU objectives: the digital single market

– One of the objectives of the digital single market is to create a framework for secure digital services and to promote user trust for the purpose of developing e.g. e-commerce, innovations, and in turn jobs and growth (point 1.1 of the explanatory memorandum).
– The proposal for a regulation under discussion is also intended to effect a form of harmonisation between the texts and to ensure coherence between Member States.
– Every three years, the Commission will carry out an evaluation of the regulation, the findings of which are to be presented to the European Parliament, the Council and the European Economic and Social Committee (Article 28).

5. General comments

5.1 The Committee welcomes the fact that a coherent package of rules is being put in place simultaneously throughout the EU to protect the rights of natural and legal persons linked to the usage of digital data by means of electronic communications.

5.1.1 It welcomes the fact that the Union is playing its role as advocate of the public's and consumers' rights.

5.1.2 It stresses that, while we are aiming for harmonisation, interpretation of many of the concepts falls to the Member States, and this is turning the regulation into a sort of directive, which leaves a great deal of room for the marketing of private data. The domain of health in particular provides an open door for the collection of huge quantities of private data.

5.1.3 Articles 11(1), 13(2), 16(4) and (5), and 24 are provisions that could be described as "transposition" provisions which would be appropriate for a directive, but not for a regulation. Operators are allowed too much leeway for the purposes of improving the quality of services (Article 5 and 6). This proposal should be an integral part of the proposal for the European Electronic Communications Code directive (COM(2016) 590 final).

5.1.4 The EESC regrets very much that these texts are entangled and voluminous, such that it is unlikely anyone other than a select few will ever read them. In effect, it is necessary to constantly go back and forth between them. Moreover their added value is not evident to the public. The fact that the proposal is difficult to read and highly complex runs counter to the spirit of the Regulatory Fitness and Performance (REFIT) programme, and to the "Better Regulation" objective; it will make it difficult to interpret and will create loopholes in the protection arrangements.

5.1.5 For example, the proposed regulation contains no definition of the concept of “operator”; for this it is necessary to refer to the draft European Electronic Communications Code[4], which has not yet entered into force and which will modify the rules of the sector as part of the single digital market, namely framework directive 2002/21/EC, the "authorisation" directive 2002/20/EC, the "universal service" directive 2002/22/EC, and the "access" directive 2002/19/EC, as amended; and to Regulation (EC) 1211/2009 setting up the Body of European Regulators for Electronic Communications (BEREC), the radio spectrum decision 676/2002/EC, Decision 2002/622/EC establishing a group on radio spectrum policy, and Decision 243/2012/EU setting up a multiannual radio spectrum policy programme (RSPP). The main reference remains of course the GDPR (see point 2.2 above), which the proposal in hand aims to complement and to which it is therefore subsidiary.

5.2 The EESC in particular stresses the content of Article 8 concerning the protection of the information stored in the terminal equipment and the potential exceptions, fundamental because it leaves to the information society opportunities for access to private data, and to that of Article 12 on presentation and restriction of calling and connected line identification. These articles are difficult for the average reader to understand.

5.2.1 The 1995 directive (Article 2) defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')". The regulation in hand, which broadens data protection to include metadata, will henceforth apply to natural as well as legal persons. It is important to reiterate that the purpose of the proposal is twofold: on the one hand to protect personal data and on the other to ensure free movement of electronic communications data, equipment and services in the EU (Article 1).

5.2.2 The EESC stresses that the will to protect the data of natural persons (Article 1(2)) will clash with other texts where such will is absent: nowhere is it clearly said that this will have to apply to those cases (see GDPR, data in the European institutions, etc.).

5.3 The EESC is wondering whether the real aim of this proposal is not to place more emphasis on its Article 1(2), namely to guarantee "the free movement of electronic communications data and electronic communications services within the Union", which shall be neither restricted nor prohibited for reasons related to respect for the private life and communications of natural and legal persons, rather than actually guaranteeing that which is announced in its Article 1(1), namely "the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data".

5.4 Everything is based on the person – natural or legal – expressing their consent. As a consequence, in the EESC's view, users must be informed, trained and remain cautious, because once their consent has been given, providers will be able to process content and metadata further in order to obtain as much effect and profit as possible. How many people know, before accepting them, that cookies are trackers? Priorities linked to this regulation should include the education of users, teaching them to make use of their rights, as well as anonymisation and encryption.

4 COM(2016)590 and annexes 1 to 11, 12.10.2016 – OJ C 125, 21.4.2017, p. 56.

6. Specific comments

6.1 Personal data should only be collated by bodies which themselves have very strict conditions and aiming at known and legitimate goals (GDPR).

6.2 However, the Committee again expresses regret at the fact that "the stated principles of the right to protection of personal data are qualified by an excessive number of exceptions and restrictions"[5]. The balance between freedom and security should remain the hallmark of the European Union, rather than balancing fundamental rights of individuals with industry rights. In its analysis of the proposal for a regulation (WP247, 4.4.2017, opinion 01/2017) , the Article 29 Working Party indicates in no uncertain terms that the proposal would decrease the level of protection established in the GDPR, e.g. with regard to locating terminal equipment and the lack of limitations on the scope of data collection (point 17), and the failure to introduce privacy protection by default (point 19).

6.3 Data are like an extension of a person, a "phantom identity", a "shadow-ID". The data belong to the person who generates them, but after they have been processed that person loses control over them. Each Member State remains responsible for data retention and transfer, and there is no harmonisation because of possible restrictions on rights introduced by the proposal. The Committee points to the risk of disparities resulting from the fact that such restrictions would be at the discretion of Member States.

6.4 A question arises particularly for people working in firms: to whom do the data they generate in the course of their work belong? And how will they be protected?

6.5 The monitoring set-up is not very clear[6]. Despite EDPB supervision, there do not appear to be adequate safeguards against arbitrary approaches and the time needed for proceedings to result in a penalty has not been assessed.

6.6 The EESC advocates the creation of a European portal where all the European and national texts, rights, appeals procedures, case law and practical aspects are brought together in one place and kept up to date so as to help the public at large and consumers find their way through the maze of texts and practices so they can exercise their rights. This portal should, at least, be based on the requirements of Directive (EU) 2016/2102 of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies, and the principles set out in recitals 12, 15 and 21 of the proposed directive known as the European Accessibility Act (2015/0278 (COD)), and provide content that is accessible and understandable to all end users. The EESC would be willing to be involved in the process of designing this portal.

6.7 In Article 22 there is no reference to "class actions", as the EESC already pointed out in its opinion on the European electronic communications code.

---

5 OJ C 125, 21.4.2017, p. 56 and OJ C 110, 9.5.2006, p. 83.

6 Chapter IV of the regulation in hand refers to the provisions of Chapter VII, in particular Article 68 GDPR.

6.8 The limitation of the substantive scope (Article 2 (2)), extension of the powers to process data without the owner's consent (Article 6(1) and (2)), the unlikely notion of obtaining the consent of *all* end-users concerned (Article 6(3)(b) and Article 8(1), (2) and (3)), and the restrictions which Member States may place on rights if they deem this to be "necessary, adequate and proportionate" are all rules whose substance is susceptible to so many interpretations that they end up running counter to the idea of genuine protection of privacy. Particular attention should also be paid to data protection relating to minors.

6.9 The EESC welcomes the right to control electronic communications covered in Article 12, but would highlight the particularly obscure wording, which seems to favour the use of telephone calls with hidden caller identity, as if anonymity were a recommendation, whereas the principle should be that the calling line can be identified.

6.10 Unsolicited communications (Article 16) and direct marketing have already been dealt with in the directive on unfair trading practices[7]. The default arrangements should be based on opting in (acceptance) rather than opting out (refusal).

6.11 The Commission's evaluation is scheduled every three years. In the digital world, that is too long. After two evaluations, the digital landscape will have changed completely. However delegation (Article 25), which will be able to be expanded, should be limited in time, and possibly renewable.

6.12 Legislation must preserve users' rights (Article 3 TEU) while guaranteeing the legal stability needed for commercial activity. The EESC regrets that the movement of data from machine to machine (M2M) is not mentioned in the proposal; reference has to be made to the European Electronic Communications Code (proposal for a directive, Articles 2 and 4).

6.12.1 The internet of things (IoT)[8] is going to lead to "big data", then to "huge data", and finally to "all data". This is a key for future waves of innovation. And machines, large or small, communicate and transmit private data between each other (e.g. information from your watch or the heartbeat data that it records and sends to your doctor's computer). Many digital players have launched their own platforms reserved for connected devices: Amazon, Microsoft, Intel and, in France, Orange and La Poste.

6.12.2 In daily life the IoT can easily be subject to malicious intrusion; the quantity of personal information which can be collected remotely is on the increase (geolocation, health data, video and audio streaming). Breaches in data protection interest for instance insurance companies, who are beginning to encourage their clients to equip themselves with connected devices and to take responsibility for their behaviour.

6.13 Many internet giants are trying to turn their original applications into platforms: thus we should distinguish the Facebook application from the Facebook platform, which allows developers to

7 OJ L 149, 11.6.2005, p. 22, Articles 8 and 9.

8 WP247/17, 1.4.2017, point 19; OJ C 12, 15.1.2015, p. 1.

devise accessible applications based on user profiles. Amazon was itself a specialised web application in online sales. Nowadays it has become a platform which allows third parties - from individuals to large groups - to market their products by benefiting from Amazon's resources: reputation, logistics, etc. All this entails the transfer of personal data.

6.14 The sharing economy is seeing a proliferation of platforms: "an intermediary platform – which is usually electronic – to put a significant number of people offering goods or services in touch with a significant number of users"[9]. While they are sought for the activity and the jobs they bring, the EESC is wondering how the data transfer they generate will be able to be controlled, in application of both the GDPR and this regulation.

Brussels, 5 July 2017.

Georges Dassis
The president of the European Economic and Social Committee

_____

9 OJ C 125, 21.4.2017, p. 56.